

# PETERBOROUGH YOUTH SERVICES

## POLICY AND PROCEDURES

<b>SECTION: ADMINISTRATION</b>	<b>POLICY NUMBER: A - 50</b>
Information Systems Management	<b>APPROVED or REVISED: APRIL 12, 2017</b>
<b>APPLIES TO: ALL</b>	<b>REVIEWED: OCTOBER 20, 2021</b>

### **POLICY**

The electronic information system includes, but is not limited to computers, networks, printers, copiers, electronic mail, electronic information and data, cell phones, and Internet access.

### **Staff Conduct**

By using Peterborough Youth Services' electronic information system, staff, contract workers, placement students and volunteers assume personal responsibility for their appropriate use and agree to comply with this policy and applicable legislation. Penalties for infractions can include loss of system access or staff discipline.

### **Systems Security**

Peterborough Youth Services takes measures to protect the integrity of systems and data and to ensure systems security, including the security of email communications.

### **PROCEDURE**

#### **Staff, Contract Workers, Placement Student and Volunteer Conduct**

Any activity that violates the following general standards for the acceptable use of computer resources is forbidden.

- Responsible behaviour with respect to the electronic information environment at all times.

- Behaviour consistent with the mission of Peterborough Youth Services.
- Compliance with all applicable laws, regulations and Peterborough Youth Services policies.
- Respect for the rights and property of others.
- Behaviour consistent with the privacy and integrity of electronic networks, electronic data and information.

## **System Security**

The Executive Director, or designate, is responsible for the maintenance and security of information systems. Any future changes made to software, electronic storage, data systems or the website will meet or exceed the security standards of those in use at the time of approval (noted below). The agency takes the following measures to protect the integrity of systems and data and to ensure systems security:

- Clients may be communicated with by text or email for scheduling purposes only. Cell phones used to contact clients are required to be password protected.
- Each staff member has access to voice mail which can only be retrieved through using a password determined by the employee. Passwords are recorded by a designated administrative staff person and stored in a secure location. The main answering machine is also accessed by password.
- All computers are password protected. Passwords are recorded by a designated administrative staff person and stored in a secure location. Computers are housed in offices that are locked during non-business hours.
- Documents containing confidential information that are being sent via email will be password protected.
- All outgoing faxes indicate that they are private and confidential. Incoming faxes are put in staff mailboxes that are in a locked filing cabinet.
- Transportation of client information through the use of portable electronic storage (e.g., USB, external hard drives) is not permitted.

- Communication with clients using an employee's personal devices or accounts (email, cell phone, social media account) is not permitted.
- Personal communications from agency devices or accounts is not permitted.
- Peterborough Youth Services' website is SSLed in order to protect the security of the website.
- The agency uses Norton Anti-Virus and the software is fully updated on an annual basis.
- The agency uses secure email servers through Go Daddy and information is stored using Office 365 (cloud services).
- The agency uses EMHware which is considered a class "A" military grade data centre, with user and group security policies and access, and has SSL web access with secure login.

